IPSec VPN Client

and the

RouteFinder® RF850/RF860

Setup Examples

Reference Guide

IPSec VPN Setup Client and the RouteFinder 850/860 Setup Examples
Reference Guide
PN S000433B Revision B

Copyright © 2007-2008
This publication may not be reproduced, in whole or in part, without prior expressed written permission from Multi-Tech Systems, Inc. All rights reserved.

Multi-Tech Systems, Inc. makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Multi-Tech Systems, Inc. reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Multi-Tech Systems, Inc. to notify any person or organization of such revisions or changes.

Revision	Date	Description
A	04/05/07	Initial release with RouteFinder software 3.32. Updated the Technical Support contract list.
B	05/07/08	Updated for software 3.34 and some minor edits.

Trademarks
The Multi-Tech logo is a registered trademark of Multi-Tech System, Inc. Windows is a trademark of Microsoft. All other trademarks are owned by their respective companies.

World Headquarters
Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, Minnesota 55112
Phone: 763-785-3500 or 800-328-9717
Fax: 763-785-9874
Internet Address: http://www.multitech.com

Technical Support

Country	By Email	By Phone
Europe, Middle East, Africa:	support@multitech.co.uk	+44 118 959 7774
U.S., Canada, all others:	support@multitech.com	800-972-2439 or 763-717-5863

Contents

Chapter 1 – Non-NAT IPSec and RouteFinder Setup Example 4
Set Up a VPN Client Using IPSec VPN Client Software and a RouteFinder 4

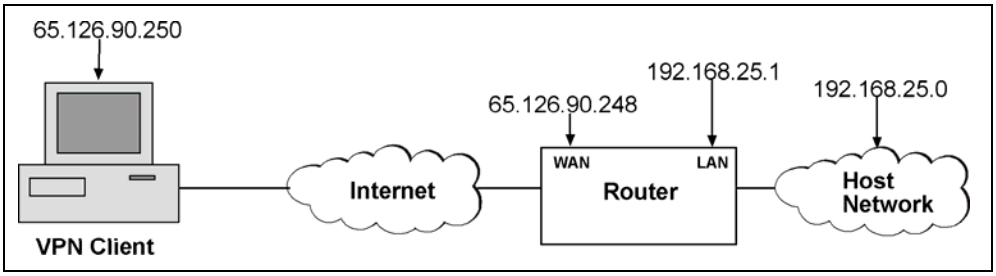
Chapter 2 – NAT Setup Example with IPSec and RouteFinder 10
Set Up a VPN Client Using IPSec VPN Client Software and a RouteFinder 10

Chapter 3 – A Reference Table of Commonly Supported Subnets 17

Chapter 1 – Non-NAT IPSec and RouteFinder Setup Example

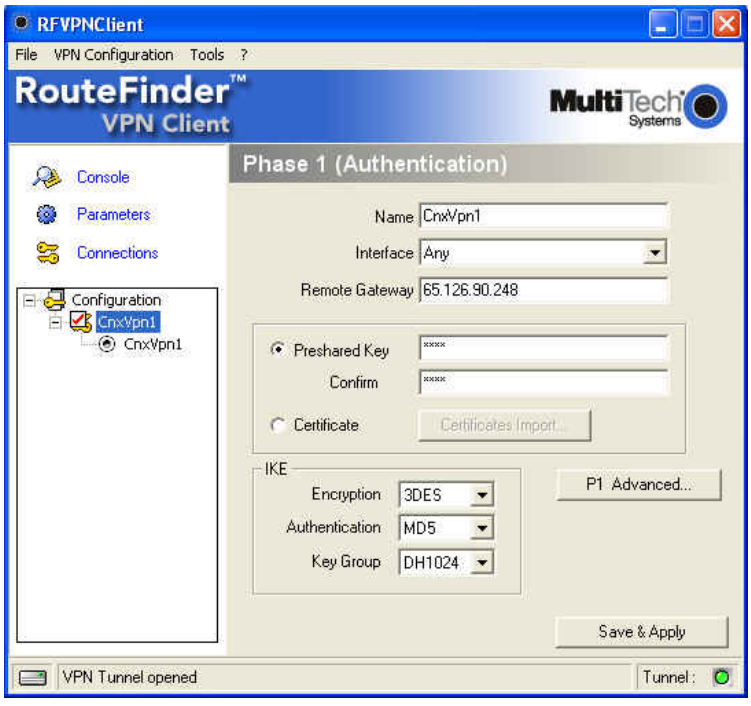
Set Up a VPN Client Using IPSec VPN Client Software and a RouteFinder

First, in this non-NAT example, set up the VPN client using the IPSec VPN Client software. Then set up the VPN tunnel for the RouteFinder using the RouteFinder software.



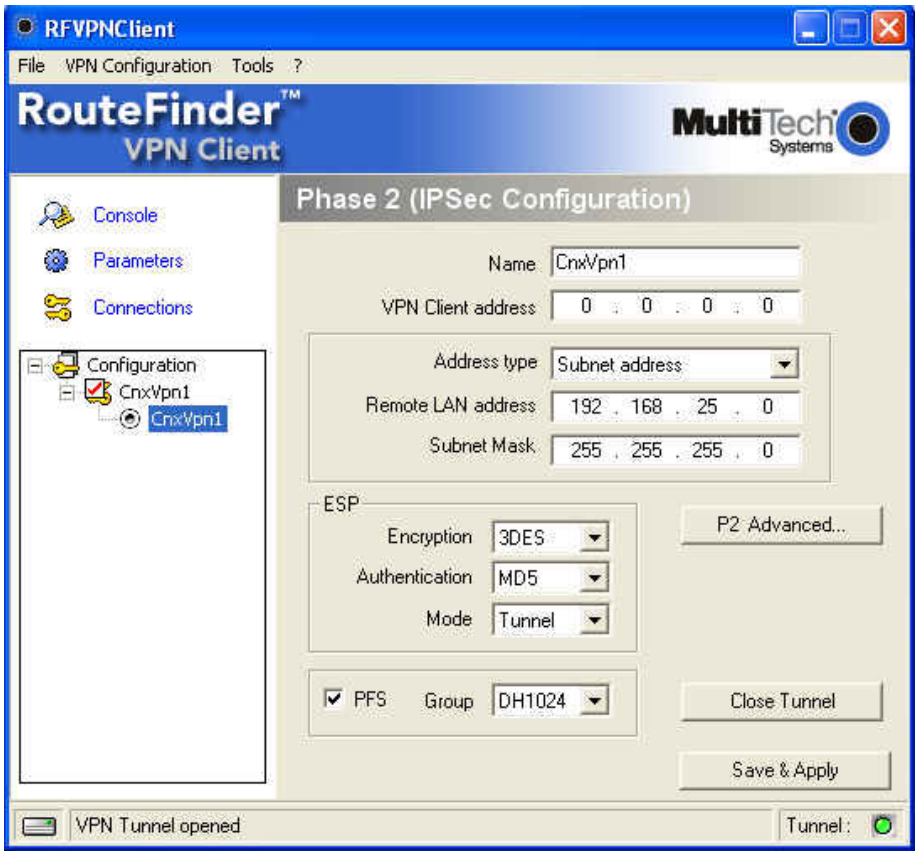
Step 1 – VPN Client Side Set Up (Phase 1)

1. Open the IPSec VPN Client software.
2. Right click on RouteFinder Client **VPN Configuration** and select **New Phase 1**.
3. Enter a name for your connection in the **Name** field.
4. Choose **Any** for the client Interface if your IP address is dynamic or the IP address provided by your ISP if Static (e.g., 65.126.90.250).
5. In the **Remote Gateway** field, enter the IP address of the VPN WAN for your Remote Gateway (e.g., 65.126.90.248).
6. Enter the Shared Secret in **Preshared Key** for your network (the Secret has to match on both ends). Then **Confirm** the shared secret by retyping the shared secret.
7. For **IKE Authentication** choose **MD5**.
8. For **Key Group** choose **DH1024**.

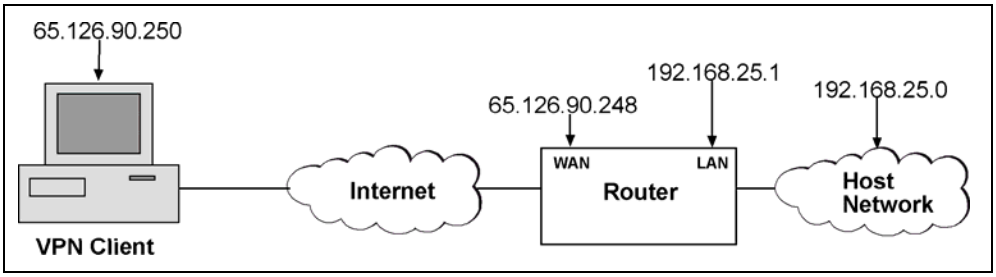


Step 2 – VPN Client Side Set Up (Phase 2)

1. Start Phase 2 by right clicking on the name of your VPN Client you created in Phase 1.
2. The **VPN Client address** will be set to 0.0.0.0 unless you have a Static IP address (e.g., 65.126.90.250).
3. The **Address type** is the type of setup on the host side. If it's a **network**, then choose **Subnet address** from the drop down list box and enter the **Remote LAN address** (e.g., 192.168.25.0) and the **Subnet Mask** (e.g., 255.255.255.0). If it's a **single IP address,** change it to that address.
4. For **ESP Authentication** choose **MD5**.
5. Accept the default **Tunnel Mode**.
6. For **PFS Group** choose **DH1024**.



Step 3 – Set Up a RouteFinder



Step 3.1 – Network & Services › Network

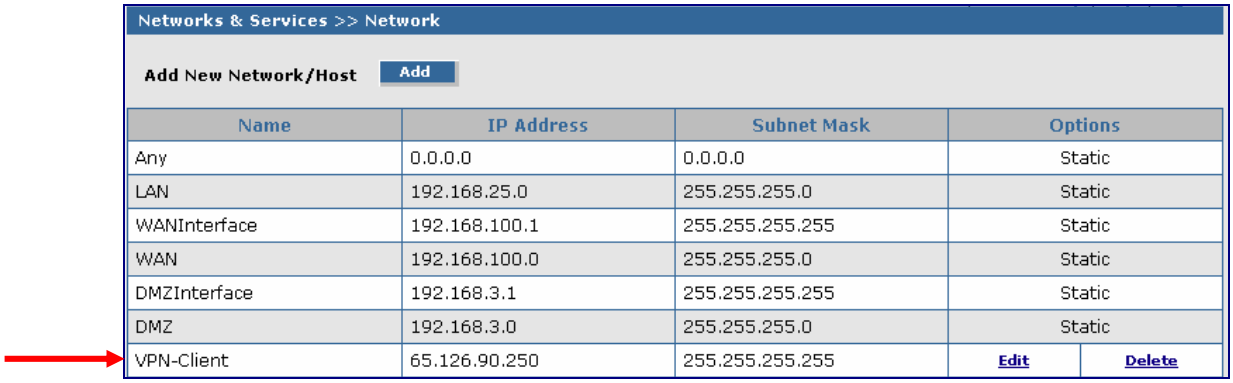
1. Login to your RouteFinder software and go to the **Networks & Services > Network** screen.
2. Click the **Add** button to open the fields for entering your network information.
3. Create a new network name for the VPN Client by entering a **Name**, **IP Address**, and **Subnet Mask**. For this example, enter the following:

   Name: VPN-Client

   IP Address: 65.126.90.250

   Subnet Mask: 255.255.255.255

   Note: The same address/mask pair should not be present in the current list displayed on the screen.
4. Click the **Add** button to add "VPN-Client" to the network list. It will display at the bottom of the screen.



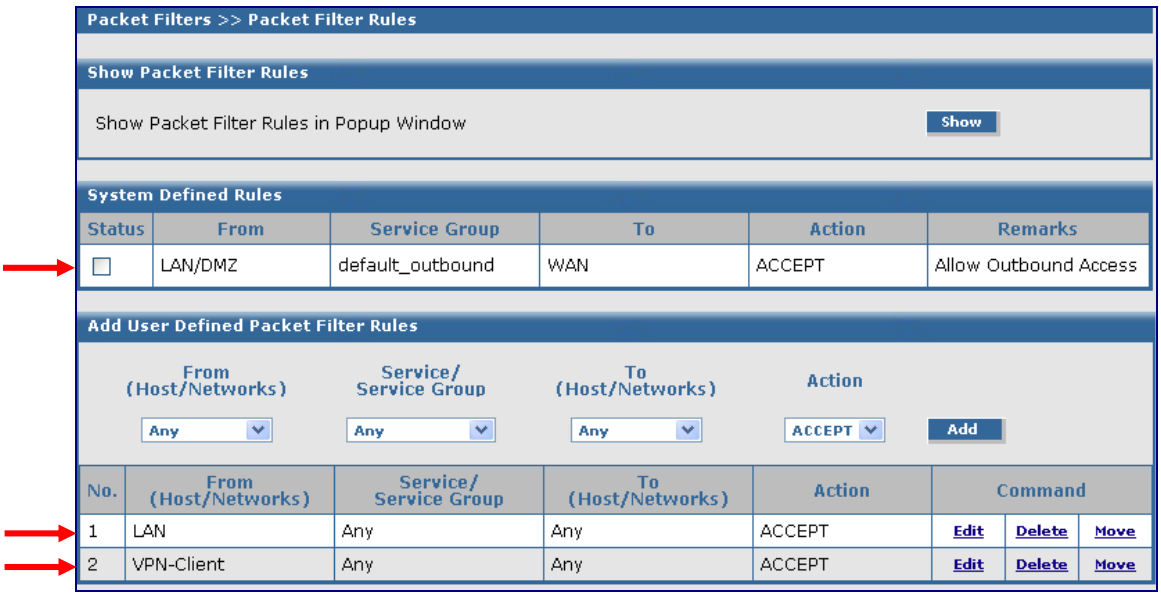
Name	IP Address	Subnet Mask	Options	
Any	0.0.0.0	0.0.0.0	Static	
LAN	192.168.25.0	255.255.255.0	Static	
WANInterface	192.168.100.1	255.255.255.255	Static	
WAN	192.168.100.0	255.255.255.0	Static	
DMZInterface	192.168.3.1	255.255.255.255	Static	
DMZ	192.168.3.0	255.255.255.0	Static	
VPN-Client	65.126.90.250	255.255.255.255	Edit	Delete

Step 3.2 – Packet Filters

1. Go to the **Packet Filters** screen to set the VPN client so it has right to access your network. The Packet Filter rights established on this screen give the client access across the tunnel to your host network.
2. In the *System Defined Rules* section, uncheck the **Status** box, if a check mark is present.
3. In the *Add User Defined Packet Filter Rules* section, click on **From (Host/Networks)** and select the network to be allowed.
   In this example, select **VPN-Client**.
4. If you are not restricting the type of Service, select **Any**.
5. If you are not restricting any Network, click on **To (Host/Network)**, and select **Any**.

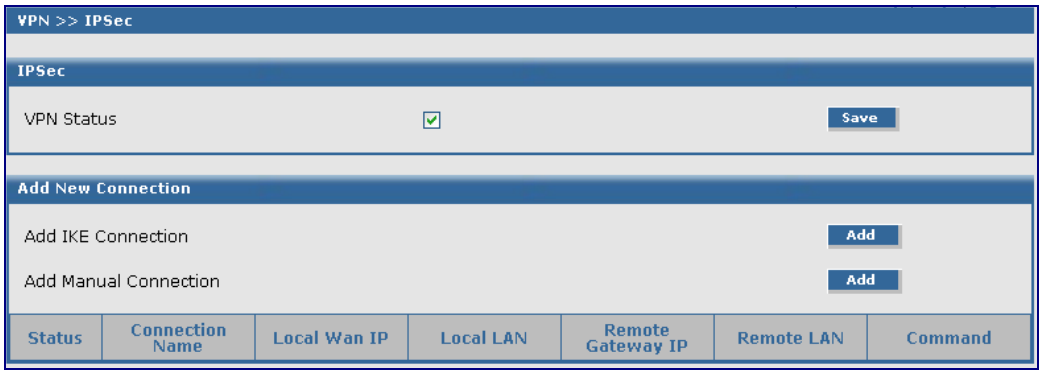
Notes:

- If the client is dynamic (unknown), set up an **Any Any Any ACCEPT** filter to allow any network to come in.
- You will need to add **LAN Any Any ACCEPT** to the *User Defined Packet Filter Rules*. If you want this rule to be in the first position so that it takes precedence over the *VPN-Client* rule, select the **Move** command, and move this rule to the first position.



Step 3.3 – VPN Setup

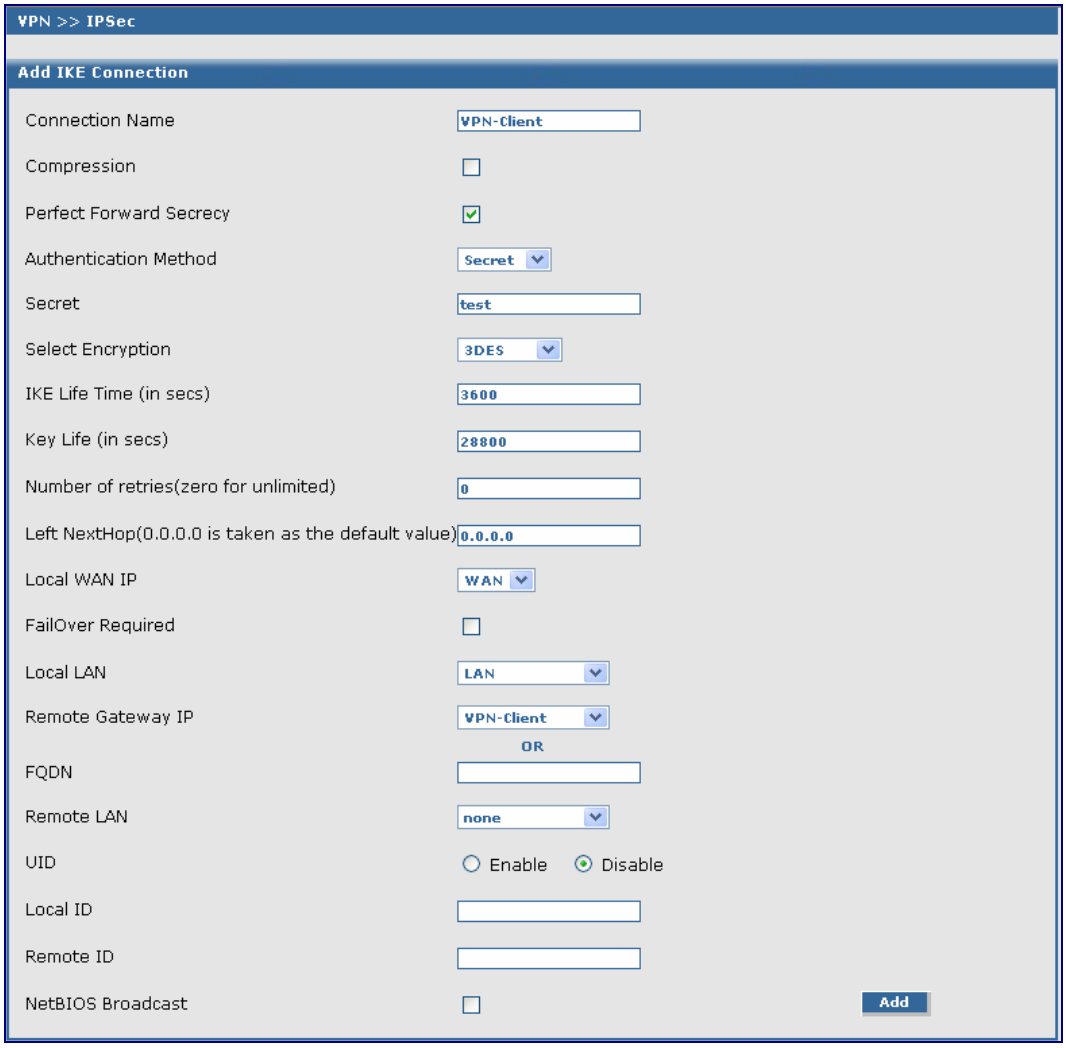
1. Go to the **VPN > IPSec** screen.
2. Click the **VPN Status** check box to enable IPSec. Then click the **Save** button.
3. Select **Add IKE Connection** by clicking the corresponding **Add** button.



Step 3.3 (Continued) – VPN Setup

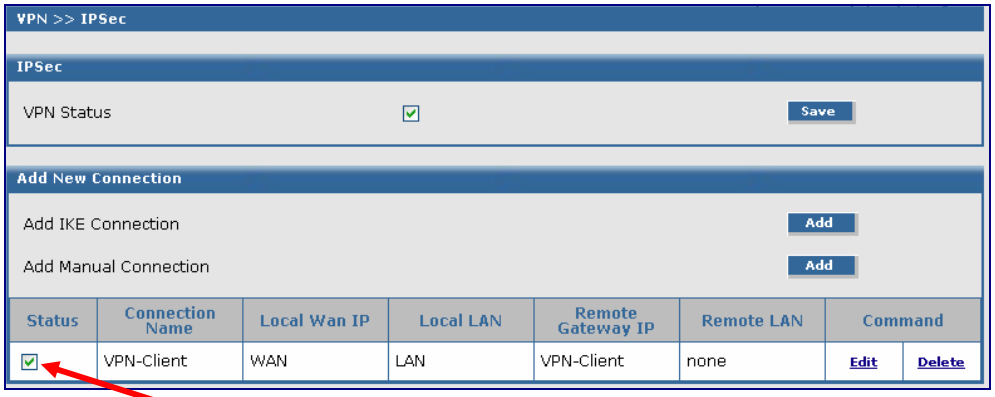
The **Add IKE Connection** screen displays. All settings can be left at the default unless otherwise indicated:

1. **Connection Name:** Enter in the name of the VPN tunnel you want to create. For this example, enter **VPN-Client**.
2. **Secret:** Enter a password (this secret password has to match on both ends of the tunnel). For this example, enter **test.**
3. **Select Encryption:** Select **3DES**.
4. **Local WAN IP:** Select **WAN**
5. **Local LAN:** Select **LAN**
6. **Remote Gateway IP:** Select **VPN-Client**.
7. **Remote LAN:** Select **None**.
8. Click the **Save** button to save your tunnel.



Step 3.3 (Continued) – VPN Setup

The VPN Status screen displays; this time with the newly-created VPN tunnel showing on the bottom of the screen.



Important Note:
Make sure to check the **Status** box for this VPN tunnel in order to activate it.

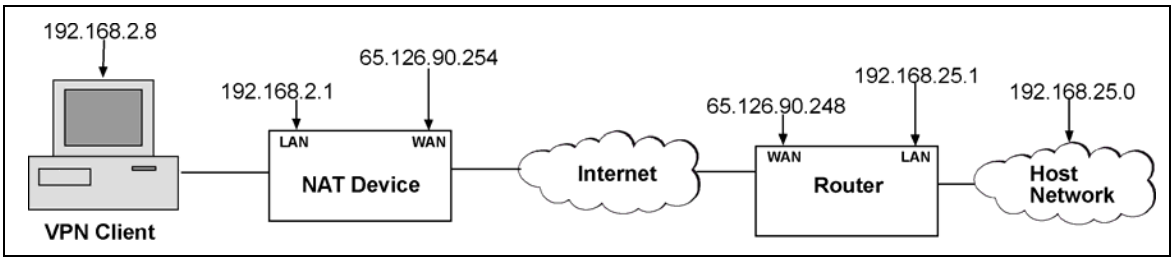
Step 4 – Checking the Tunnel

To see if the tunnel is up you can click on **Statistics & Logs** and go to the **IPSec > IPSec Live Connections**. You will see whether or not the connection is up. You will also see information about the data, if any, that is being sent across the tunnel.

Chapter 2 – NAT Setup Example with IPSec and RouteFinder

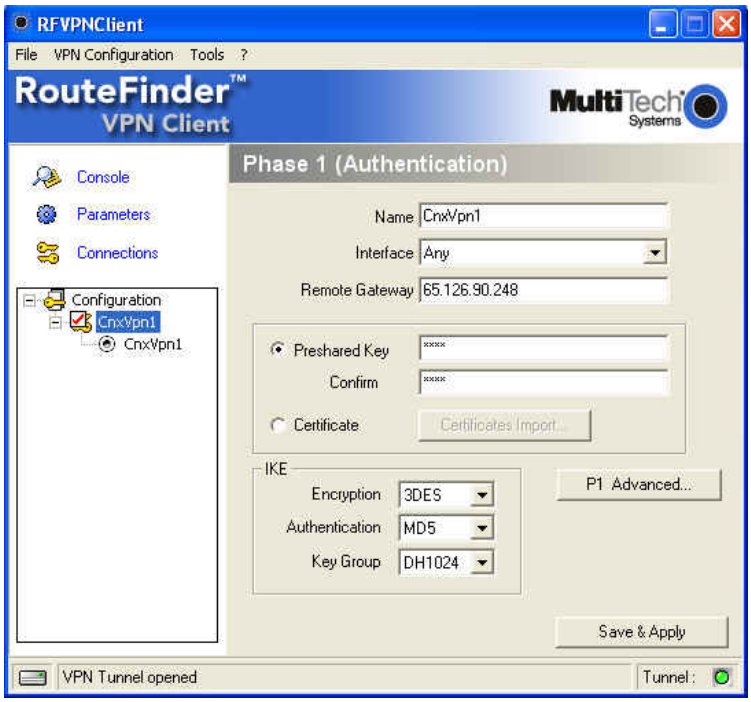
Set Up a VPN Client Using IPSec VPN Client Software and a RouteFinder

First, in this NAT example, set up the VPN client in the IPSec VPN Client software. Then set up the VPN tunnel for the RouteFinder using the RouteFinder software.



Step 1 – VPN Phase 1 Client Setup (Behind NAT)

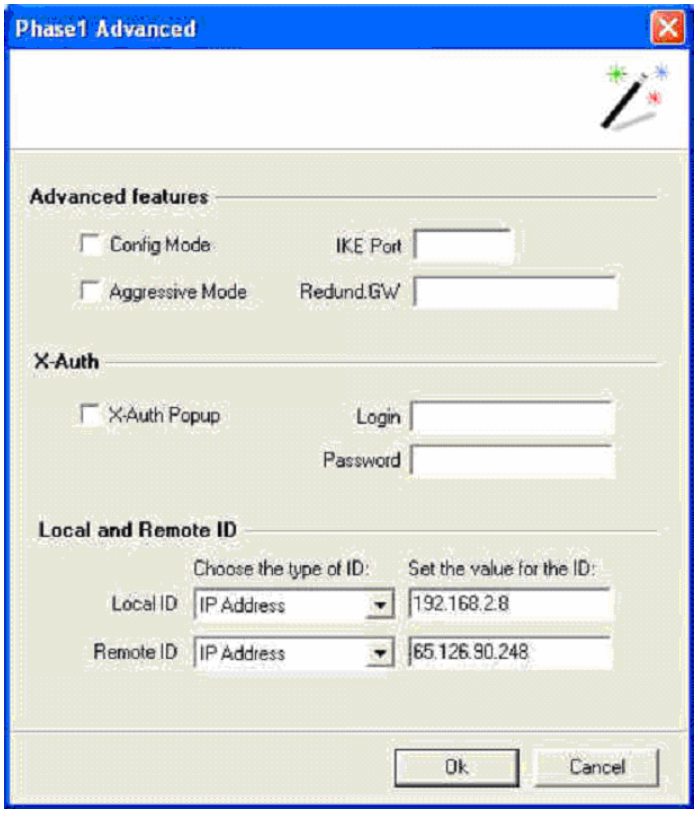
1. Open the IPSec VPN Client software.
2. Right click on RouteFinder Client **VPN Configuration** and select **New Phase 1**.
3. Enter the name of your connection in the **Name** field.
4. Choose **Any** for the client **Interface** if your IP address is dynamic or the if the IP address is provided by your LAN (a Static IP Address). Example: 198.168.2.8.
5. Enter the IP address of the VPN WAN for your **Remote Gateway**. Example: 65.126.90.248.
6. Enter the Shared Secret in **Preshared Key** for your network (the secret has to match on both ends). Then **Confirm** the shared secret by entering the Shared Secret again.
7. For **IKE Authentication** choose **MD5**.
8. For **Key Group** choose **DH1024**.
9. Click the **P1 Advanced** button.



Step 2 – Client Phase 1 Advanced Setup (Behind NAT)

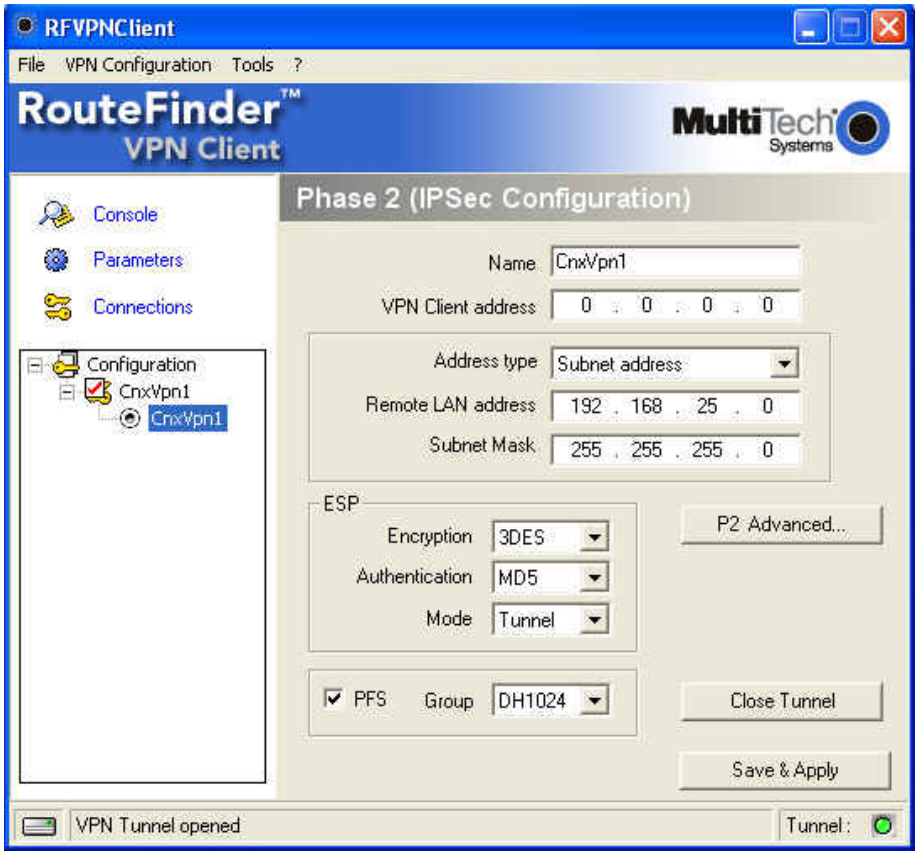
This screen displays after clicking the **P1 Advanced** button on the previous screen.

1. Select the **IP Address** from the drop down list box for the **Local ID.**
2. Then enter the IP address of the VPN Client in the text box labeled ***Set the value for the ID*** field. Example: 192.168.2.8
3. Select **IP Address** for the **Remote ID.**
4. Then enter the IP address of the RouteFinder in the ***Set the value for the ID*** field. Example: 65.126.90.248
5. Click **OK**.

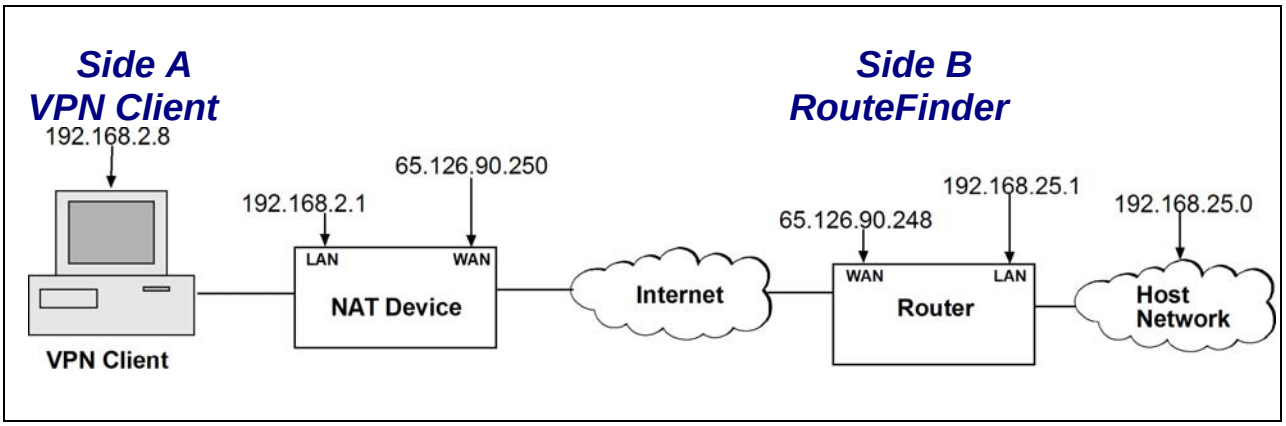


Step 3 – Client Phase 2 Setup (Behind NAT)

1. Start Phase 2 by right clicking on the name of your VPN Client created in Phase 1.
2. The **VPN Client address** will be set to 0.0.0.0 unless you have a Static IP address. Example: 192.168.2.8.
3. The **Address type** is the type of setup on the host side. If it's a **network**, then choose **Subnet address** and enter the Remote LAN address (Ex. 192.168.25.0) and the Subnet Mask (Ex. 255.255.255.0). If it's a **single IP address**, change it to that address.
4. For **ESP Authentication** choose **MD5**.
5. Click **OK**.



Step 4 – Set Up a RouteFinder (Side B)



Step 4.1 – Networks & Services › Network

1. Login to your RouteFinder and go to the **Networks & Services > Network** screen.
2. Click the **Add** button to open the fields for entering your network information.
3. Create a new network name for the VPN-Client by entering a **Name**, **IP Address**, and **Subnet Mask**. For this example, enter the following:

   Name: VPN-Client

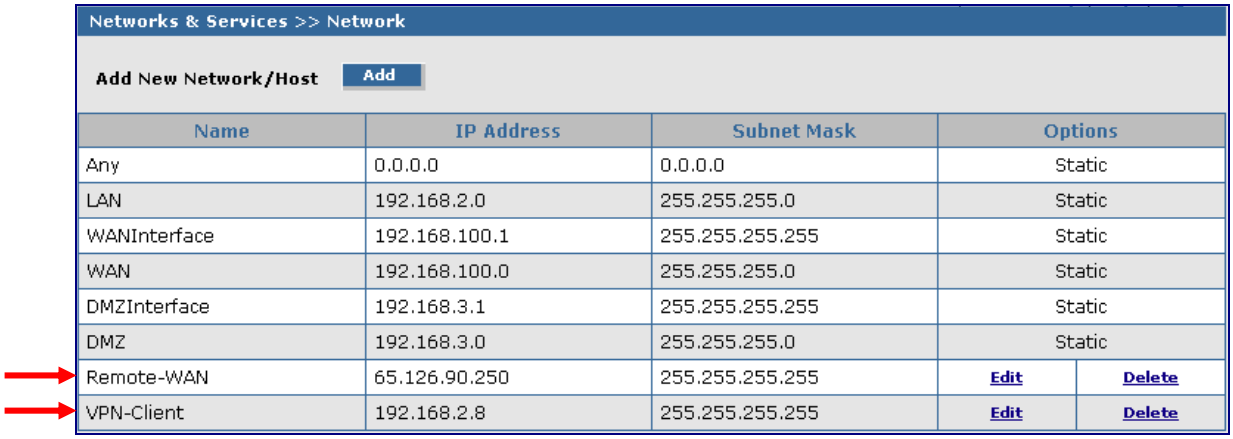
   IP Address: 192.168.2.8

   Subnet Mask: 255.255.255.255
4. Click the **Add** button to add the network to the list.
5. Create a new network name for the Remote WAN by entering a **Name**, **IP Address**, and **Subnet Mask**. For this example, enter the following:

   Name: Remote-WAN

   IP Address: 65.126.90.250

   Subnet Mask: 255.255.255.255

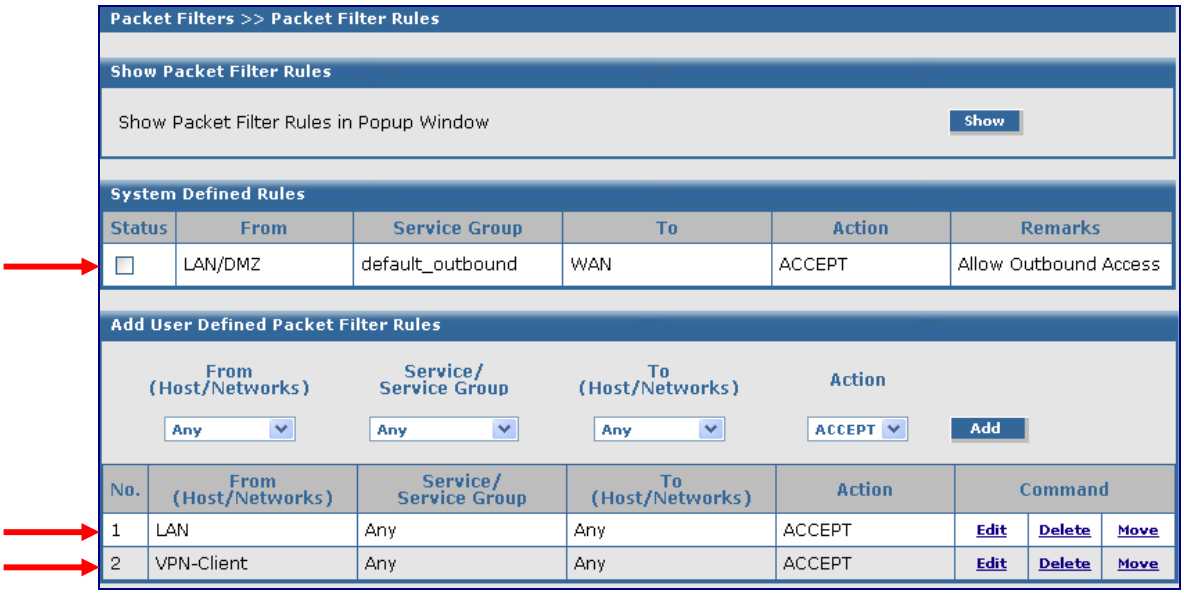


Step 4.2 – Packet Filters

1. Go to the **Packet Filters** screen to set the VPN client tunnel rights. The Packet Filter rights established on this screen give the client access across the tunnel to your host network.
2. In the *System Defined Rules* section, uncheck the **Status** box, if a check mark is present when you are adding User Defined Packet Filter Rules.
3. In the *Add User Defined Packet Filter Rules* section, click on **From (Host/Networks)** and select the network to be allowed.
   In this example, select **VPN-Client**.
4. If you are not restricting the type of Service, select **Any**.
5. If you are not restricting any Network, click on **To (Host/Networks)**, and select **Any**.

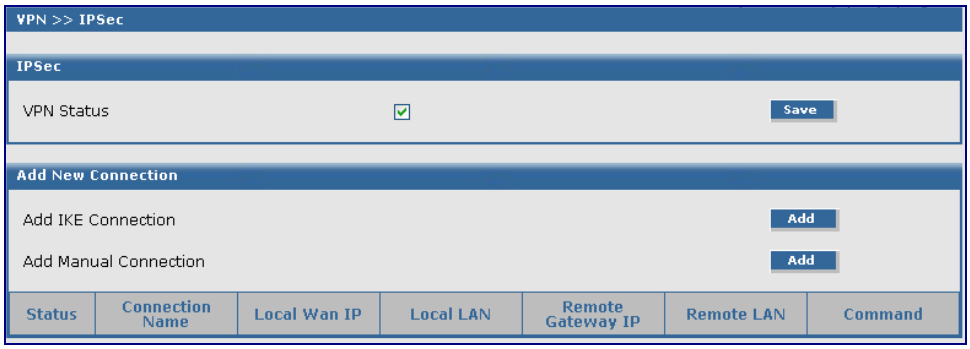
Notes:

- If the client is dynamic (unknown), set up an **VPN-Client Any Any ACCEPT** filter to allow any network to come in.
- You will have to add **LAN Any Any ACCEPT** to the *User Defined Packet Filter Rules*. If you want this rule to be in the first position so that it takes precedence over the *VPN-Client* rule, select the **Move** command, and move this rule to the first position.



Step 4.3 – VPN Setup

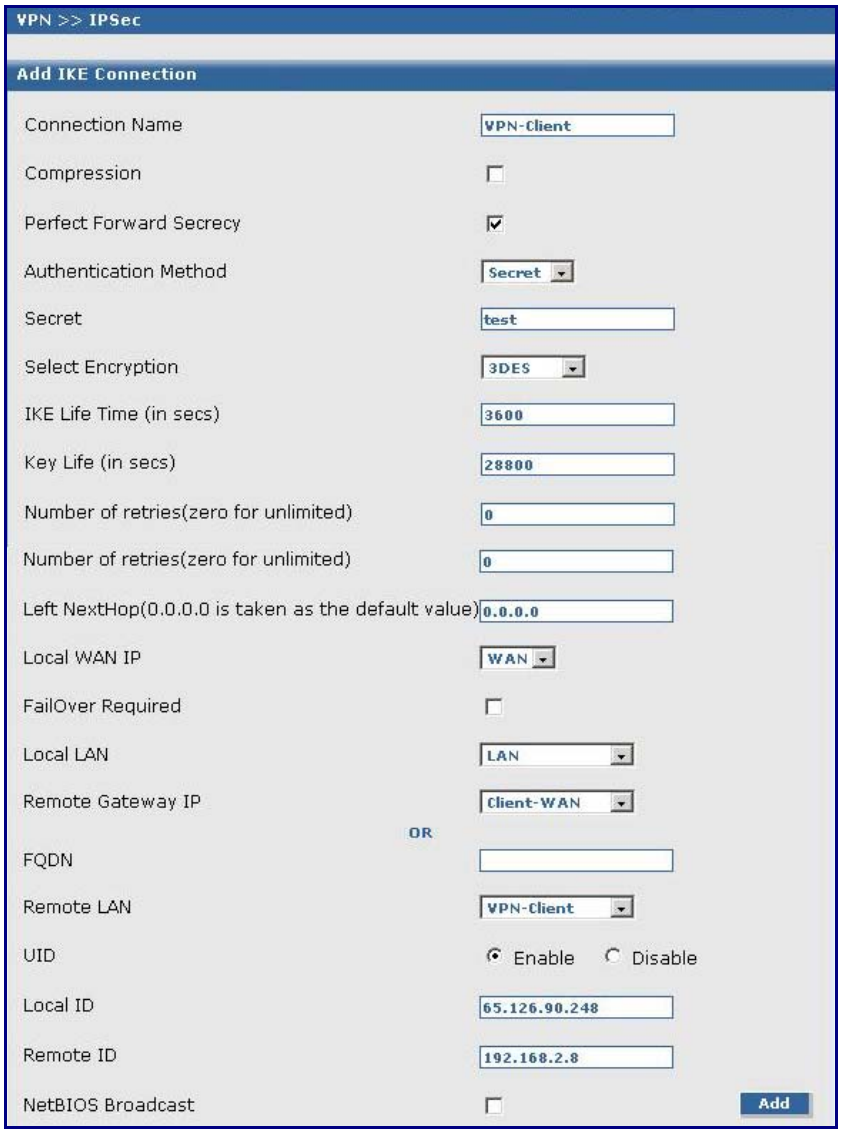
1. Go to the **VPN > IPSec** screen.
2. Click on the **VPN Status** check box to enable IPSec. Then click the **Save** button.
3. Select **Add IKE Connection** by clicking the corresponding **Add** button.



Step 4.3 (Continued) – VPN Setup

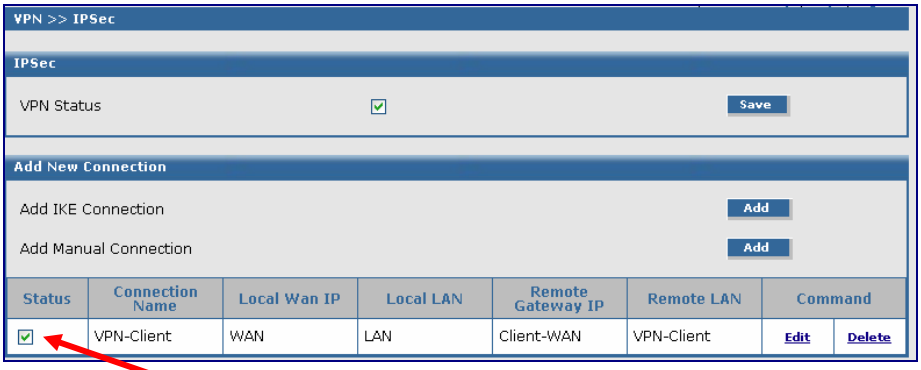
The **Add IKE Connection** screen displays. All settings can be left at the default unless otherwise indicated:

1. **Connection Name:** Enter the name of the VPN tunnel you want to create. For this example, enter **VPN-Client**.
2. **Secret:** Enter the **Secret** password (which has to match on both ends of the tunnel). For this example, enter **test**.
3. **Select Encryption:** Select **3DES**.
4. **Local WAN IP:** Select **WAN**.
5. **Local LAN:** Select **LAN**.
6. **Remote Gateway IP:** Select **Client-WAN**.
7. **Remote LAN:** Select **VPN-Client**.
8. **UID:** Select **Enable**.
9. **Local ID** (the RouteFinder WAN Address)**: 65.126.90.248**
10. **Remote ID** (the client PC Address)**: 192.168.2.8**
11. Click the **Save** button to save your tunnel settings.



Step 4.3 (Continued) – VPN Setup

The **VPN > IPSec** screen now displays the VPN connection at the bottom of the screen.



Note:
Make sure to check the **Status** box at the bottom of the screen on the left side to activate the newly created tunnel.

Step 4 – Checking the Tunnel

To see if the tunnel is up you can click on **Statistics & logs** and go to the **IPSec > IPSec Live Connections**. You will see the connection up; and if any data is being sent across, you will see that information here.

Chapter 3 – A Reference Table of Commonly Supported Subnets

This table lists commonly supported Subnets organized by Address.

	Network Number	Hosts Available	Broadcast Address
255.255.255.128	N.N.N.0	N.N.N.1-126	N.N.N.127
/25	N.N.N.128	N.N.N.129-254	N.N.N.255

	Network Number	Hosts Available	Broadcast Address
255.255.255.192	N.N.N.0	N.N.N.1-62	N.N.N.63
/26	N.N.N.64	N.N.N.65-126	N.N.N.127
	N.N.N.128	N.N.N.129-190	N.N.N.191
	N.N.N.192	N.N.N.193-254	N.N.N.255

	Network Number	Hosts Available	Broadcast Address
255.255.255.224	N.N.N.0	N.N.N.1-30	N.N.N.31
/27	N.N.N.32	N.N.N.33-62	N.N.N.63
	N.N.N.64	N.N.N.65-94	N.N.N.95
	N.N.N.96	N.N.N.97-126	N.N.N.127
	N.N.N.128	N.N.N.129-158	N.N.N.159
	N.N.N.160	N.N.N.161-190	N.N.N.191
	N.N.N.192	N.N.N.193-222	N.N.N.223
	N.N.N.224	N.N.N.225-254	N.N.N.255

	Network Number	Hosts Available	Broadcast Address
255.255.255.240	N.N.N.0	N.N.N.1-14	N.N.N.15
/28	N.N.N.16	N.N.N.17-30	N.N.N.31
	N.N.N.32	N.N.N.33-46	N.N.N.47
	N.N.N.48	N.N.N.49-62	N.N.N.63
	N.N.N.64	N.N.N.65-78	N.N.N.79
	N.N.N.80	N.N.N.81-94	N.N.N.95
	N.N.N.96	N.N.N.97-110	N.N.N.111
	N.N.N.112	N.N.N.113-126	N.N.N.127
	N.N.N.128	N.N.N.129-142	N.N.N.143
	N.N.N.144	N.N.N.145-158	N.N.N.159
	N.N.N.160	N.N.N.161-174	N.N.N.175
	N.N.N.176	N.N.N.177-190	N.N.N.191
	N.N.N.192	N.N.N.193-206	N.N.N.207
	N.N.N.208	N.N.N.209-222	N.N.N.223
	N.N.N.224	N.N.N.225-238	N.N.N.239
	N.N.N.240	N.N.N.241-254	N.N.N.255

	Network Number	Hosts Available	Broadcast Address
255.255.255.248	N.N.N.0	N.N.N.1-6	N.N.N.7
/29	N.N.N.8	N.N.N.9-14	N.N.N.15
	N.N.N.16	N.N.N.17-22	N.N.N.23
	N.N.N.24	N.N.N.25-30	N.N.N.31
	N.N.N.32	N.N.N.33-38	N.N.N.39
	N.N.N.40	N.N.N.41-46	N.N.N.47
	N.N.N.48	N.N.N.49-54	N.N.N.55
	N.N.N.56	N.N.N.57-62	N.N.N.63
	N.N.N.64	N.N.N.65-70	N.N.N.71
	N.N.N.72	N.N.N.73-78	N.N.N.79
	N.N.N.80	N.N.N.81-86	N.N.N.87
	N.N.N.88	N.N.N.89-94	N.N.N.95
	N.N.N.96	N.N.N.97-102	N.N.N.103
	N.N.N.104	N.N.N.105-110	N.N.N.111
	N.N.N.112	N.N.N.113-118	N.N.N.119
	N.N.N.120	N.N.N.121-126	N.N.N.127
	N.N.N.128	N.N.N.129-134	N.N.N.135
	N.N.N.136	N.N.N.137-142	N.N.N.143
	N.N.N.144	N.N.N.145-150	N.N.N.151
	N.N.N.152	N.N.N.153-158	N.N.N.159
	N.N.N.160	N.N.N.161-166	N.N.N.167
	N.N.N.168	N.N.N.169-174	N.N.N.175
	N.N.N.176	N.N.N.177-182	N.N.N.183
	N.N.N.184	N.N.N.185-190	N.N.N.191

	N.N.N.192	N.N.N.193-198	N.N.N.199
	N.N.N.200	N.N.N.201-206	N.N.N.207
	N.N.N.208	N.N.N.209-214	N.N.N.215
	N.N.N.216	N.N.N.217-222	N.N.N.223
	N.N.N.224	N.N.N.225-230	N.N.N.231
	N.N.N.232	N.N.N.233-238	N.N.N.239
	N.N.N.240	N.N.N.241-246	N.N.N.247
	N.N.N.248	N.N.N.249-254	N.N.N.255

	Network Number	**Hosts Available**	**Broadcast Address**
255.255.255.252	N.N.N.0	N.N.N.1-2	N.N.N.3
/30	N.N.N.4	N.N.N.5-6	N.N.N.7
	N.N.N.8	N.N.N.9-10	N.N.N.11
	N.N.N.12	N.N.N.13-14	N.N.N.15
	N.N.N.16	N.N.N.17-18	N.N.N.19
	N.N.N.20	N.N.N.21-22	N.N.N.23
	N.N.N.24	N.N.N.25-26	N.N.N.27
	N.N.N.28	N.N.N.29-30	N.N.N.31
	N.N.N.32	N.N.N.33-34	N.N.N.35
	N.N.N.36	N.N.N.37-38	N.N.N.39
	N.N.N.40	N.N.N.41-42	N.N.N.43
	N.N.N.44	N.N.N.45-46	N.N.N.47
	N.N.N.48	N.N.N.49-50	N.N.N.51
	N.N.N.52	N.N.N.53-54	N.N.N.55
	N.N.N.56	N.N.N.57-58	N.N.N.59
	N.N.N.60	N.N.N.61-62	N.N.N.63
	N.N.N.64	N.N.N.65-66	N.N.N.67
	N.N.N.68	N.N.N.69-70	N.N.N.71
	N.N.N.72	N.N.N.73-74	N.N.N.75
	N.N.N.76	N.N.N.77-78	N.N.N.79
	N.N.N.80	N.N.N.81-82	N.N.N.83
	N.N.N.84	N.N.N.85-86	N.N.N.87
	N.N.N.88	N.N.N.89-90	N.N.N.91
	N.N.N.92	N.N.N.93-94	N.N.N.95
	N.N.N.96	N.N.N.97-98	N.N.N.99
	N.N.N.100	N.N.N.101-102	N.N.N.103
	N.N.N.104	N.N.N.105-106	N.N.N.107
	N.N.N.108	N.N.N.109-110	N.N.N.111
	N.N.N.112	N.N.N.113-114	N.N.N.115
	N.N.N.116	N.N.N.117-118	N.N.N.119
	N.N.N.120	N.N.N.121-122	N.N.N.123
	N.N.N.124	N.N.N.125-126	N.N.N.127
	N.N.N.128	N.N.N.129-130	N.N.N.131
	N.N.N.132	N.N.N.133-134	N.N.N.135
	N.N.N.136	N.N.N.137-138	N.N.N.139
	N.N.N.140	N.N.N.141-142	N.N.N.143
	N.N.N.144	N.N.N.145-146	N.N.N.147
	N.N.N.148	N.N.N.149-150	N.N.N.151
	N.N.N.152	N.N.N.153-154	N.N.N.155
	N.N.N.156	N.N.N.157-158	N.N.N.159
	N.N.N.160	N.N.N.161-162	N.N.N.163
	N.N.N.164	N.N.N.165-166	N.N.N.167
	N.N.N.168	N.N.N.169-170	N.N.N.171
	N.N.N.172	N.N.N.173-174	N.N.N.175
	N.N.N.176	N.N.N.177-178	N.N.N.179
	N.N.N.180	N.N.N.181-182	N.N.N.183
	N.N.N.184	N.N.N.185-186	N.N.N.187
	N.N.N.188	N.N.N.189-190	N.N.N.191
	N.N.N.192	N.N.N.193-194	N.N.N.195
	N.N.N.196	N.N.N.197-198	N.N.N.199
	N.N.N.200	N.N.N.201-202	N.N.N.203
	N.N.N.204	N.N.N.205-206	N.N.N.207
	N.N.N.208	N.N.N.209-210	N.N.N.211
	N.N.N.212	N.N.N.213-214	N.N.N.215
	N.N.N.216	N.N.N.217-218	N.N.N.219
	N.N.N.220	N.N.N.221-222	N.N.N.223
	N.N.N.224	N.N.N.225-226	N.N.N.227
	N.N.N.228	N.N.N.229-230	N.N.N.231
	N.N.N.232	N.N.N.233-234	N.N.N.235
	N.N.N.236	N.N.N.237-238	N.N.N.239
	N.N.N.240	N.N.N.241-242	N.N.N.243
	N.N.N.244	N.N.N.245-246	N.N.N.247
	N.N.N.248	N.N.N.249-250	N.N.N.251
	N.N.N.252	N.N.N.253-254	N.N.N.255